TEXAS CYBERSECURITY STRATEGIC PLAN

FISCAL YEARS 2018-2023

OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

JANUARY 25, 2018

DIR

Texas Department of Information Resources

CONTENTS

STATE OF TEXAS CYBERSECURITY VISION STATEMENT:

The State of Texas will use its resources efficiently, collaboratively and effectively to create a risk-aware culture that places high value on protecting information entrusted to the state, and to form a protected and resilient cybersecurity environment.

FROM THE DESK OF THE CHIEF INFORMATION SECURITY OFFICER:

As the threat landscape changes, so does the defensive posture of governments tasked with protecting and securing citizen data. Increasingly complex cybersecurity challenges continually put state IT systems at risk. New attack vectors, such as the internet of things (IoT), are difficult to address with traditional tools and methods.

As stewards of cybersecurity in the public sector, state cybersecurity professionals have the important responsibility of maintaining the public's trust. We must adopt a forward-looking mindset that strives to maintain a progressive and proactive approach in our cybersecurity posture.

The mission of the Texas Cybersecurity Strategic Plan is to assist public sector security personnel in improving their organization's cybersecurity effectiveness through alignment with statewide goals. Although many organizations are mature in their cybersecurity efforts, continuous improvement is an important component of an effective cybersecurity program.

At the Texas Department of Information Resources (DIR), we strive to offer progressive planning resources for our customers. Our hope is that you incorporate the goals and actions outlined in this plan to improve your organization's cybersecurity program. The five goals discussed in this plan -- engagement, tooling, staffing, response, and outreach -- represent the critical pillars for success. Aligning your cybersecurity plan with these goals can help you and your organization be prepared to address the challenges we often face.

Recent large-scale data breaches highlight more than ever the importance of securing our citizen data, especially in a state as large as Texas. It is our responsibility as public-sector security professionals to protect and secure the sensitive and confidential information of our citizens. Although this cybersecurity plan is directed at a statewide level, it can offer your organization a foundation for strengthening your cybersecurity program.

As always, DIR and the Office of the Chief Information Security Officer are here to assist you. I hope to see many of you incorporating these goals to advance your cybersecurity initiatives. United we can defend Texas against the threats we face, and together, we will succeed.

Nancy Rainosek
Chief Information Security Officer
Texas Department of Information Resources

GOAL 1: ENGAGEMENT

FOSTER STATE AND AGENCY LEADERSHIP ENGAGEMENT FOR CYBERSECURITY INITIATIVES

OVERVIEW:

An effective cybersecurity program must be integrated into all facets of an organization. As with many other organizational outcomes, leadership engagement is crucial to the accomplishment of many cybersecurity initiatives. In recent years, state policy makers and executive leadership have become more involved in the world of cybersecurity as a result of breaches or exposures affecting their organizations and similar cyber events reported in the news. While this is a step in the right direction, cybersecurity staff need to continue the conversation with decision-makers regarding the issues affecting the cybersecurity landscape and the impact it can have on daily operations and business activities.

CHALLENGE:

Often, executives do not become fully engaged in the organization's cybersecurity program until after a business-impacting incident has occurred. This reactive approach to cybersecurity management can result in slow program maturity development, as staff are preoccupied by tactical matters instead of proactively assessing and preparing organizations to face future challenges.

ACTIONS:

- Communicate the risks and benefits of the organization's cybersecurity initiatives with state leadership and agency executive management in financial and operational terms.
- Ensure that the Information Security Officer provides executive management with assessments which are free from any organizational constraints.
- Utilize a standardized reporting framework to consistently communicate security posture to agency leadership.
- Participate in cybersecurity advocacy groups to identify common pain points that can be addressed through rule or statute.
- Encourage and provide opportunities for executive management to attend cybersecurity training to better understand cybersecurity risks.

OUTCOMES:

Short Term: Leadership understands the cybersecurity challenges and risks, including those acknowledged in their Agency's Security Plan, and allocates resources to improve the cybersecurity posture.

Long Term: Stronger cybersecurity programs with a culture of awareness by addressing major concerns throughout all levels of state government.

67% of agency business-role personnel

VS.

77% of IT-role personnel

STRONGLY AGREED CYBERSECURITY IS IMPORTANT TO AGENCY FUNCTIONS

SOURCE: 2017 IT Planning Leadership Survey

GOAL 2: TOOLING

PROVIDE PROACTIVE CYBERSECURITY DEFENSE THROUGH INSIGHT AND TECHNOLOGY

OVERVIEW:

With better protection, monitoring, and alerting, an agency is better able to respond quickly and efficiently to cyber threats. Artificial intelligence, machine learning, network forensic tools, and other technologies are innovative approaches that offer potential benefits that, if implemented appropriately, may greatly improve an agency's security program effectiveness. However, different tools have their own strengths and weaknesses. To obtain the most comprehensive view of the threats facing an organization, multiple tools and strategies must be implemented.

CHALLENGE:

Implementing the latest-and-greatest technologies, while appealing, can be difficult due to the technical, cultural, and financial impacts of the technology. Obtaining funding for new technologies is often challenging in a government budget and funding cycle that emphasizes cost reduction and efficiencies within existing operations. The increasing complexity and volume of threats present additional challenges in timely implementation of effective tools.

ACTIONS:

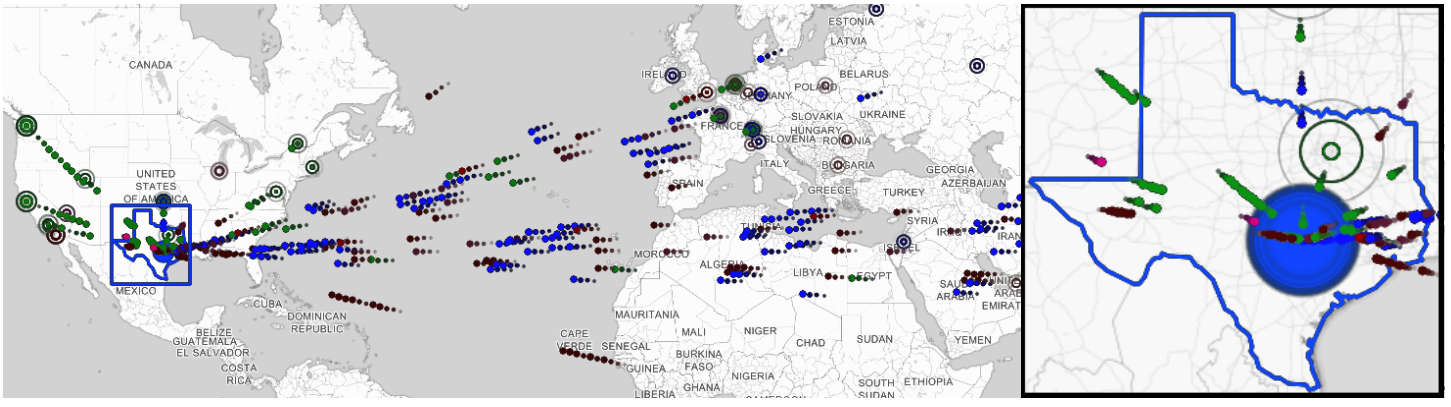
- Evaluate new and emerging technologies to address evolving threats and continue to advocate for cost-efficient, effective, and scalable solutions.
- Partner with agencies experienced in prospective technologies to obtain greater insight, lessons learned, and determine suitability for the agency.
- Evaluate whether the Managed Security Services program would be an appropriate fit for the agency's information security needs
- Develop vendor criteria documentation to determine ability to meet regulatory requirements and minimum acceptable standards.

OUTCOMES:

Short Term: Improved systems protection and threat identification, reduced incident response times, and greater insight into the threat landscape that can impact business operations.

Long Term: Security programs that keep up with current technologies and reduced risk of adverse cybersecurity events.

Threat Map (below): In a moment's time, Texas faces hundreds of cyber attacks from all over the world.



GOAL 3: STAFFING

ENSURE ADEQUATE KNOWLEDGE, SKILLS, AND EXPERIENCE OF THE CYBERSECURITY WORKFORCE

OVERVIEW:

People are the most important resource in any security operation. In the State of Texas, projected employment growth for information security analysts from 2014 to 2024 is greater than 30% , higher than the estimated national growth of 18%. With cyber incidents making headlines across the country, it is not surprising that demand for talented professionals has increased dramatically. To compound these challenges, the increasing sophistication of threats requires highly skilled individuals who are in demand in both the public and private sectors.

CHALLENGE:

Competition between the public and private sector for skilled cybersecurity professionals leaves state government at a disadvantage when it comes to attracting and retaining high-caliber staff. To address this challenge, agencies should attempt to develop creative ways to attract, train, and retain qualified staff, leveraging existing programs to meet their cybersecurity staffing needs.

ACTIONS:

- Partner with education institutions to attract students to cybersecurity, and investigate internship programs.
- Ensure current staff have the necessary skills and abilities to combat cyberthreats by maintaining current training and certifications.
- Conduct job analysis on security staff to ensure job titles and descriptions match job functions, thereby increasing the effectiveness of the selection process.
- Develop creative retention programs that incentivize career development and advancement in the field of cybersecurity.

OUTCOMES:

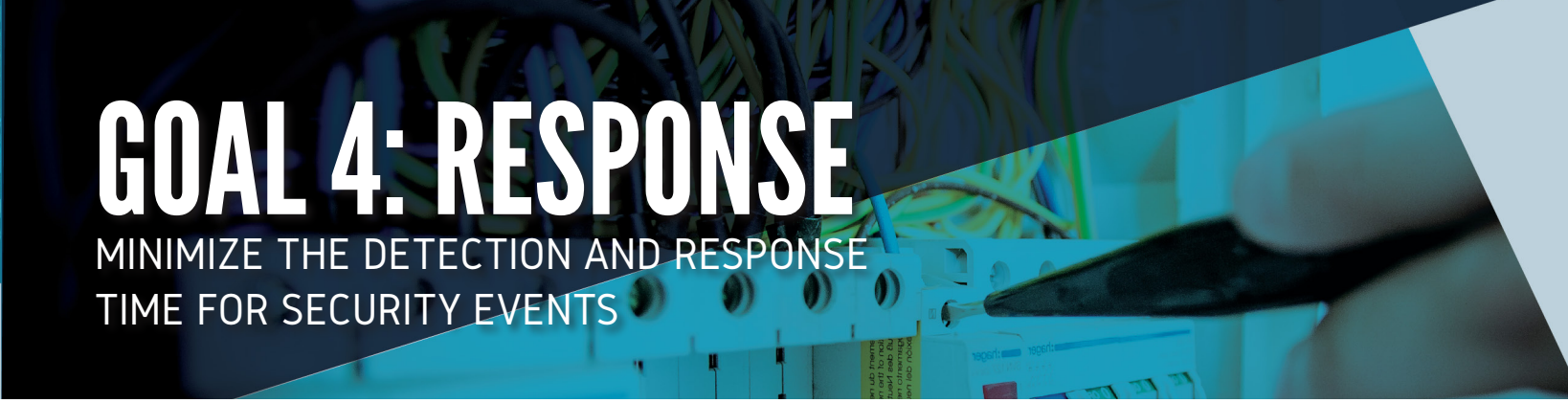
Short Term: More clearly defined cybersecurity roles and responsibilities with potential for increased staff development.

Long Term: Resilient security program defined by a stable workforce with the ability and expertise to respond quickly and efficiently.

Count of dedicated Information Security personnel in the state of Texas

Fiscal Year	FTEs (rounded)	% Growth
2013	54	
2014	71	33%
2015	89	25%
2016	112	26%
2017	142	26%

SOURCE: Texas State Auditor's Office



GOAL 4: RESPONSE

MINIMIZE THE DETECTION AND RESPONSE TIME FOR SECURITY EVENTS

OVERVIEW:

Large breaches or exposure of confidential information and emerging cybersecurity threats are becoming more frequent. It is critical that agencies are prepared to respond to such events to ensure that essential business processes are not slowed or stopped due to an incident, and more importantly, that citizen data is not compromised. Therefore, it is crucial that agencies identify areas of improvement in their incident response plans before an adverse impact occurs. Adequate detection capabilities improve the ability to discover a breach quickly as well as provide the information necessary to respond quickly and thoroughly.

CHALLENGE:

Successful incident response occurs when the issue is properly identified, the resources are available to address it, and prioritized solutions are implemented. Incident response capabilities vary from organization to organization. Some agencies have more resources than others to deal with security incidents. Many organizations do not regularly test their incident response plans, thus when a security incident occurs, the organization may learn it is not adequately prepared to address the incident.

ACTIONS:

- Increase intelligence sharing through situational awareness reports.
- Participate in, and contribute to, the Information Sharing and Analysis Organizations.
- Participate in cybersecurity and incident response exercises to improve overall response and communications between state agencies.
- Facilitate and improve incident response effectiveness.
- Establish clear escalation procedures within the organization and the state as a whole.

OUTCOMES:

Short Term: Clearer understanding of appropriate actions to perform and individuals to engage regarding cybersecurity incident management.

Long Term: Decreased time between event occurrence and detection, between detection and response, and reduced severity of incidents through more effective incident response processes.

INTERNAL DETECTION OF COMPROMISE OCCURRED IN LESS THAN 20% OF ALL THE REPORTED BREACHES

WITHIN THE PUBLIC ADMINISTRATION INDUSTRY, THE TIME FROM COMPROMISE TO DETECTION (KNOWN AS DWELL TIME) WAS MEASURED IN YEARS FOR MORE THAN 50% OF THE BREACHES

SOURCE: 2016 Data Breach Investigations Report

GOAL 5: OUTREACH

ESTABLISH A CYBERSECURITY OUTREACH PROGRAM TO INCREASE AWARENESS OF CYBERSECURITY BEST PRACTICES

OVERVIEW:

End-user behavior makes up a significant portion of the State's exposure and risk. To have an effective cybersecurity program, a culture of awareness must be adopted into the values of the organization. Outreach, training, and cybersecurity awareness at all levels are critical components in risk reduction.

CHALLENGE:

Some users may not understand the importance of cybersecurity as it relates to their job responsibilities. Others may simply lack the awareness or knowledge of secure computing practices and safe web browsing. In either case, educating staff and the public can greatly reduce the success of malicious attacks.

ACTIONS:

- Routinely assess the effectiveness of cybersecurity end-user training programs.
- Participate in information sharing to foster communication among the private and public sectors.
- Investigate opportunities to engage outside communities and organizations to increase awareness of cybersecurity issues.
- Engage business areas to participate in developing effective cybersecurity awareness and training programs.

OUTCOMES:

Short Term: Increased end-user awareness of malicious campaigns resulting in fewer cyber incidents.
Long Term: A cyber-aware State of Texas capable of identifying risks to reduce overall exposure.

HAVING AN INCIDENT RESPONSE TEAM CAN SAVE AN AVERAGE OF **$19** PER DATA RECORD AND APPROXIMATELY **$457,691** PER BREACH.

PARTICIPATING IN THREAT SHARING CAN SAVE AN AVERAGE OF **$8** PER RECORD AND APPROXIMATELY **$193K** PER BREACH.

SOURCE: 2017 Ponemon Cost of Data Breach Study

SERVICE HIGHLIGHTS

POLICY & GOVERNANCE

DIR establishes baseline security standards for Texas state agencies and institutions of higher education. The standards are closely aligned to the Federal Information Security Management Act and National Institute of Standards and Technology.

SECURITY ASSESSMENTS

DIR offers comprehensive security assessments for state agencies and institutions of higher education. These security risk assessments gauge the 'health' of the organization, provide lists of strengths and weaknesses for management, and suggest a roadmap and plans to improve the security posture for the organization.

CYBERSECURITY AWARENESS & EDUCATION

As a statewide leader in information resources security, DIR provides education and support to state agencies, institutions of higher education, and local governments through a variety of methods.

NETWORK SECURITY OPERATIONS CENTER

The Network Security Operations Center (NSOC) provides 24x7 network security monitoring, alerting and analysis services to provide early warning for attempted intrusions and cyber-attacks, and to alert authorities who are responsible for deploying appropriate countermeasures. The NSOC also proactively identifies and blocks billions of unauthorized or malicious communication attempts monthly.

VULNERABILITY SCANS/ PENETRATION TESTING

Penetration Tests and Web Application Vulnerability Scans are performed on agency networks and web domains to identify vulnerabilities. The results of the tests are provided to the agency personnel for remediation.

DATA CENTER SERVICES PROGRAM

The state data centers enable Texas state agencies and institutions of higher education to share data center infrastructure, reduce focus on IT infrastructure operations and concentrate on their core business while strengthening security, enhancing disaster recovery and managing costs. There are currently more than forty-five state agencies, three institutions of higher education and three non-state agencies utilizing the Data Center Services program.

ANNUAL INFORMATION SECURITY FORUM

The Information Security Forum is a free educational conference aimed at city, county and state Information Security Officers throughout the state of Texas.

LEGACY MODERNIZATION

DIR has developed a strategy to guide the state in legacy system modernization efforts. The strategy includes guiding plans for modernization of legacy systems statewide and at the agency level; assisting the legislature by providing prioritization of legacy modernization and cybersecurity funding requests; and establishing a statewide application development framework.

STATEWIDE PORTAL FOR ENTERPRISE CYBERSECURITY THREAT, RISK AND INCIDENT MANAGEMENT (SPECTRIM)

To help tie together the overall state security program, DIR has implemented a governance, risk and compliance software tool available to all state agencies and institutions of higher education. The SPECTRIM portal provides incident management and analysis, policy management, risk assessment analysis and security plan preparation.

LOOKING FORWARD

MANAGED SECURITY SERVICES (MSS)

The MSS model establishes a select set of voluntary security services provided to state agencies by service providers that are united by DIR through a Master Service Integrator (MSI) to provide cohesive delivery and value-added components. The MSS program will assist agencies in meeting legislative requirements, mitigating security risks, and filling gaps in skill sets necessary to provide a secure computing environment for each agency and institution of higher education. Included in these offerings will be device management, incident response, and risk and compliance.

CYBER STORM VI

DIR will be leading a group of Texas state agencies participating in Cyber Storm VI which will be held in April 2018. Cyber Storm is a biennial exercise sponsored by the Department of Homeland Security and provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind. Congress has mandated the Cyber Storm exercise series to strengthen cyber preparedness in the public and private sectors.

DIR ACADEMY

The DIR Academy is designed to provide continuing education for state Information Security Officers and their staffs. The courses offered will prepare security professionals working for the state of Texas for various industry certifications.

INCIDENT RESPONSE AND THREAT SHARING

To address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible. DIR is developing plans for a Texas Information Sharing and Analysis Organization to share threat and incident information and provide services to improve the incident response capabilities.

ACKNOWLEDGEMENTS

TEXAS CYBERSECURITY STRATEGIC PLANNING COMMITTEE

Mike Bell, Texas Department of Criminal Justice

Terri Duncan, Texas Department of Transportation

Shirley Erp, Health and Human Services Commission

Claudia Escobar, Office of the Attorney General

Dan Fletcher, Health Professions Council

Paul Hopingardner, City of Austin

Bekir Kitis, Texas Department of Transportation

Randy Lott, Travis County

Helen Mohrmann, University of Texas System

David Morgan, Department of Public Safety

Dan Owen, Texas State University

Jesse Rivera, Comptroller of Public Accounts

Brandon Rogers, General Land Office

Ed Serna, Texas Workforce Commission

Jeffrey Smith, Office of the Governor

George Stolard, General Land Office

Frosty Walker, Texas Education Agency

Texas Department of Information Resources

www.dir.texas.gov
300 West 15th St., Suite 1300
Austin, TX 78701
1-855-ASK-DIR1